

REMARKS

Claims 1-3, 6-13, 16-19, and 21-24 were pending and presented for examination and in this application. In an Office Action dated October 30, 2009, claims 1-3, 6-13, 16-19, and 21-24 were rejected. Claims 1, 10, and 21 have been amended, claims 6, 23 and 24 have been cancelled, and claims 25-27 are new. Based on the above amendments and the following Remarks, Applicants respectfully request that the Examiner reconsider all outstanding objections and rejections, and withdraw them.

REJECTIONS UNDER 35 U.S.C. § 103(a)

Claims 1, 9-10, 18-19, and 21-24 stand rejected under 35 U.S.C. § 103 as being anticipated by Moore et al. (U.S. Patent No. 7,000,015) in view of Yufik (U.S. Patent No. 5,794,224). Applicant respectfully traverses these rejections as applied to the amended claims.

The independent claims recite elements related to associating computer network identifications with network policies. For example, independent claim 1 recites the following:

1. (Currently Amended) A method for associating computer network identifications with network policies, said method comprising the steps of:
 - analyzing a network interface associated with a client computer using a plurality of network detectors, including a first detector and a second detector, the detectors outputting a set of a plurality of netspecs, each netspec comprising a first token identifying a detector used for the analysis and a second token identifying the analyzed network interface;
 - determining that the first detector that outputs a first netspec of the set of netspecs is more reliable in observing network interfaces than the second detector that outputs a second netspec of the set of netspecs;**
 - awarding a higher priority to the first netspec in response to the first netspec being output by the first detector and the first detector being more reliable than the second detector;
 - associating the network identifications made by the first and second netspecs of the set of netspecs with locations based at least in part on the priority order of the first and second netspecs; and
 - feeding associated network identification/location pairs to a network interface module to implement desired network policies.

Similar elements are recited in independent claims 10 and 21.

As most of the restrictions of claim 24 are now incorporated into independent claims 1, 10 and 21, Applicants will address the Examiner's rejections of claim 24. The combination of Moore and Yufik do not teach all of the recited elements of the claims. Specifically, as the Examiner admits, Moore fails to disclose at least the step of **"determining that a first detector that outputs a first netspec is more reliable in observing network interfaces than a second detector that outputs a second netspec"** as recited in the amended claims. Yufik fails to remedy this deficiency.

Yufik discloses a system of resource allocation, where goals and priorities are indicated by a user in the form of network terminal nodes, and allocation decisions are made based on these goals. Yufik, Abstract. Specifically, network links between starting and terminal nodes are weighted based on the frequency and relative success of exercising the same network links in past allocation decisions. *Id.* Thus, reliability in the context of Yufik is limited to *the success of the connective capability of a network link*. *Id.*, col. 7, 63-67; col. 8, 1-5. In contrast, Claim 1 discloses determining that a network detector is reliable *in observing network interfaces*. Reliability in the context of claim 1 thus concerns the accuracy of the functional capability of the network detector. The reliability of Yufik's network links is measured in how well the links have been implemented in the past; the reliability of Claim 1's network detectors is measured in how well the detectors perform in observing network interfaces. The two measures of reliability are functionally and (as will be discussed below) compositionally distinct.

Assuming, for the sake of argument, that Moore does disclose network detectors, the combination of Moore and Yufik at best discloses a system with network detectors that allocates network resources to network links successfully utilized between two network nodes in the past. The combination fails to disclose determining the reliability of a **network detector** in observing network interfaces.

In addition, Yufik fails to disclose determining that a first network detector is more reliable in observing network interfaces than a second detector. The Examiner cites to Yufik's abstract (lines 1-13), however this passage (as mentioned above) only discloses weighting network links based on "the frequency and relative success of exercising those links in the previous allocation decisions". Yufik does not disclose determining, between two network

detectors, which is more reliable in observing network interfaces. Thus, the combination of Moore and Yufik does not disclose the claimed element **“determining that a first detector that outputs a first netspec is more reliable in observing network interfaces than a second detector that outputs a second netspec”**.

Accordingly, Applicant respectfully submits that the cited references do not teach or suggest every element of amended claims 1, 11, and 21. Therefore, the independent claims are not anticipated by the cited references, nor are anticipated the dependent claims that incorporate the elements of their base claims.

Claims 2-3, 6-8, 11-13, and 16-17 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Moore in view of Aaron (U.S. Publication No. 2004/0268150).

For at least the reasons stated above regarding why the combination of Moore and Yufik fails to disclose all of the elements of the independent claims, the combination also fails to disclose the elements of dependent claims 2-3, 6-8, 11-13, and 16-17. Aaron does not remedy the deficiencies in Moore and Yufik, as discussed in the previous Office Action Response. Aaron discloses a system for providing network-based firewall policy configuration and facilitation. *See* Aaron, Abstract. A policy modification agent (“PMA”) resides on a memory along with an operating system. *See* Aaron, [0028]. A user sends a notification to a firewall facilitation coordinator (“FFC”) to modify the user’s firewall policy for a new application. The FFC receives the notification and authenticates the user. The FFC sends a request to the PMA seeking modification of the firewall policy as applied to the new application. *See* Aaron, [0044]. Upon receiving the request, the PMA initiates an “exercise period”. During the exercise period the PMA observes packets associated with the new application. *See* Aaron, [0046]. The PMA then generates rules for filtering the packets based on whether questionable packets are observed during this exercise period. *See* Aaron, [0047]-[0050] and FIGS. 5A-5D. However, like Moore and Yufik, Aaron does not disclose determining that a first detector that outputs a first netspec is more reliable in observing network interfaces than a second detector that outputs a second netspec, nor does the Examiner claim that it does.

Thus, Moore, Yufik and Aaron, either alone or in the combination suggested by the Examiner, do not teach or suggest every element of independent claims 1, 10, and 21, nor the

claims depending therefrom. Accordingly, Applicant requests withdrawal of this rejection.

CONCLUSION

Withdrawal of the pending rejections and reconsideration of the claims are respectfully requested, and a notice of allowance is earnestly solicited. If the Examiner has any questions concerning this Response, the Examiner is invited to telephone Applicant's representative at (650) 335-7185.

Respectfully Submitted,
Peter Linhardt

Date: January 27, 2010 By: /Antonia L. Sequeira/
Antonia L. Sequeira, Esq.
Reg. No.: 54,670
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (650) 335-7185
Fax.: (650) 938-5200